



Defense Information Systems Agency

A Combat Support Agency

Assured Sharing Framework (ASF)

Accelerating innovation while managing the
residual risk

Need for Middleware

- Currently the process for new capability to be fielded within the Global Information (GIG) can take upwards of six months to three years. Before an operational evaluation time and money is spent
 - Configuring to security standards
 - Designing compensating controls
 - Meeting the requirements DoD IA business culture
 - Adhering to Open standards and interoperating with DoD data sources
- The ever changing demand of the DoD mission requires agile reaction to an ever increasing new threat
- Need for improved DoD acquisition and financing strategies for IT capabilities

Excessive sunk costs are experienced prior to understanding the true value of the capability

Strategic Importance

- Quickly expose new and emerging IT-capability to meet situational awareness
 - VCJCS and DoD CIO have expressed a need to quickly deploy capability for evaluation prior to full investment
 - Must make data available via the web for reuse in new and novel ways
- ASF provides the DoD a common protected enclave for hosting uninitiated capability
 - A protected enclave can provide the security and interoperability function for promising capability and focus funds on business needs and evaluation
 - The communication paths of the embedded web service are fully arbitrated to the GIG.
 - Capabilities have a clear migration path for standard communication and IA activities for release into the GIG

ASF supports both User interaction and Web Service Chaining

What is ASF?

- ASF provides a trusted hosting environment by meeting the C&A requirements thus establishing the IA boundary
- The ASF is a collection of COTS products and their connection to Enterprise Service to control interfaces of new un-trusted 3rd-party capabilities (web services and/or applications), thus providing the needed trust via the ASF enclave itself
 - It uses network security such as private IP's in order to prevent direct connect of the un-trusted hosted web services from connecting to the Enterprise and other hosted services
 - At the application layer, ASF arbitrates all communication between the un-trusted hosted web service and the Enterprise and other hosted service
- ASF is an enabling technology for exposing 3rd-party capabilities as web services and in itself is not an end-product for the war-fighter, only providing arbitrated access to Enterprise Infrastructure technical underpinning

A trusted hosting enclave that meets DOD's IA Culture, Open SOA standards, and arbitrates all external communications for 3rd-party capabilities

Information Assurance Pedigree

- ASF is accredited for testing (IATT expires 14 Oct 2011) on the premise that a hosted 3rd-party capability cannot be trusted
- IATO package was approved on 1 June 2011
- All Category I and II findings have been mitigated within the ASF
- 72% percent of the products (18) used within ASF have undergone NIST product certification or are in current evaluation status (5), the remaining (2) are planned
- DSAWG has approved the use of private (non-routable) IP addresses on the SIPRNet as part of layered defense-in-depth approach
- Each Capability within the ASF is individually provided data from known endpoints

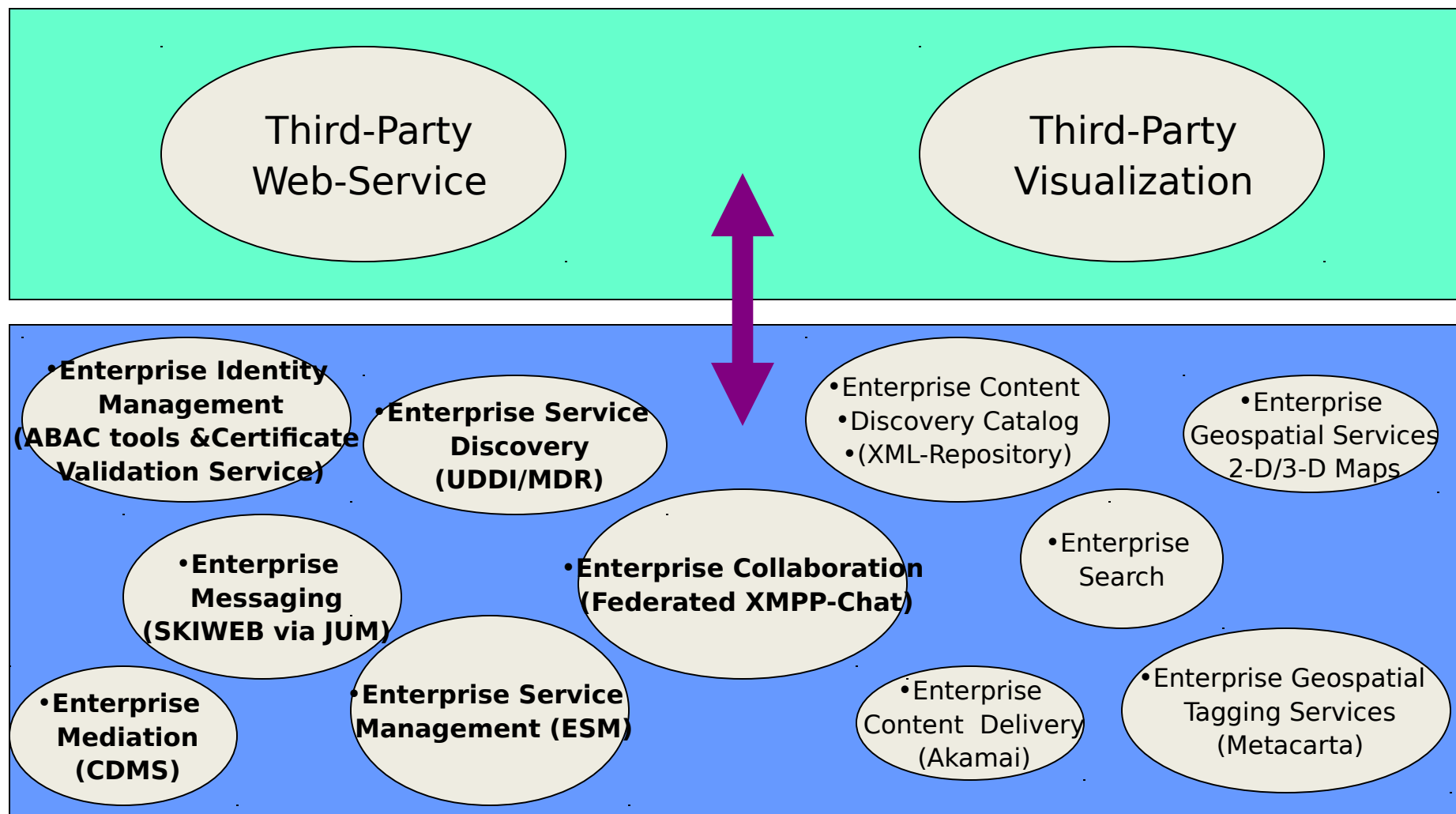
**ASF provides a new architectural component to
better secure the DoD**

Arbitrated ASF Interface Flows

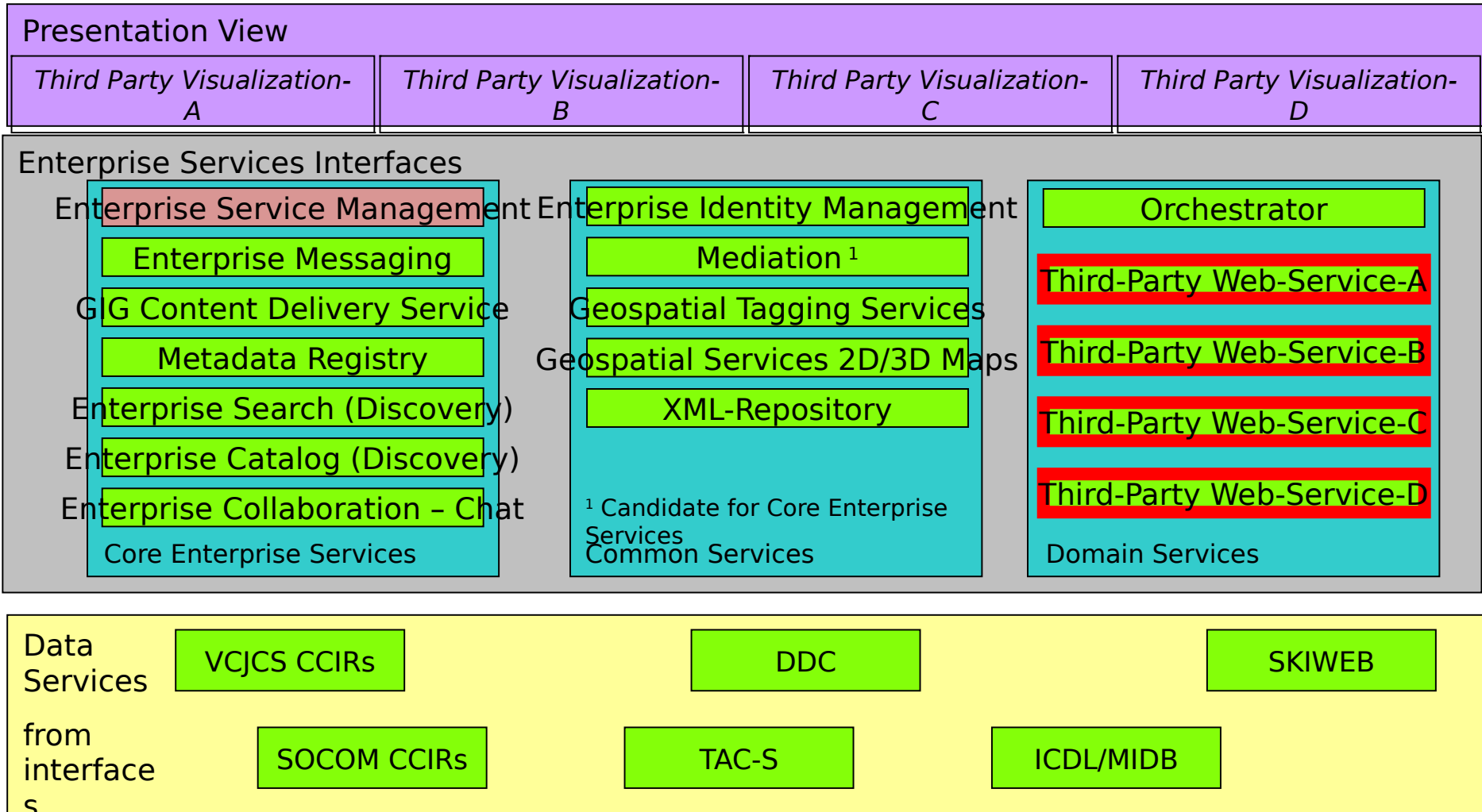
- **Implemented in ASF**
 - **Enterprise Identity Management (ABAC w/CVS)**
 - **Enterprise Messaging (SKIWEB CCIRs via JUM)**
 - **Enterprise Service Discovery (UDDI/MDR)**
 - **Enterprise Service Management (ESM) - data capture**
 - **Enterprise Collaboration (Federated XMPP-Chat) - available when DCO can federate**
 - **Enterprise Content Discovery Catalog (XML-Repository)**
 - **Enterprise Search**
 - **Enterprise Mediation (CDMS)**
- *What could be added in the future*
 - *Enterprise Content Delivery Service (Akamai)*
 - *Enterprise Geospatial Services (2-D/3-D Maps)*
 - *Enterprise Geospatial Tagging Services (Metacarta)*

Most Enterprise Service Interfaces available – securely

Leveraging Critical Enabling Services



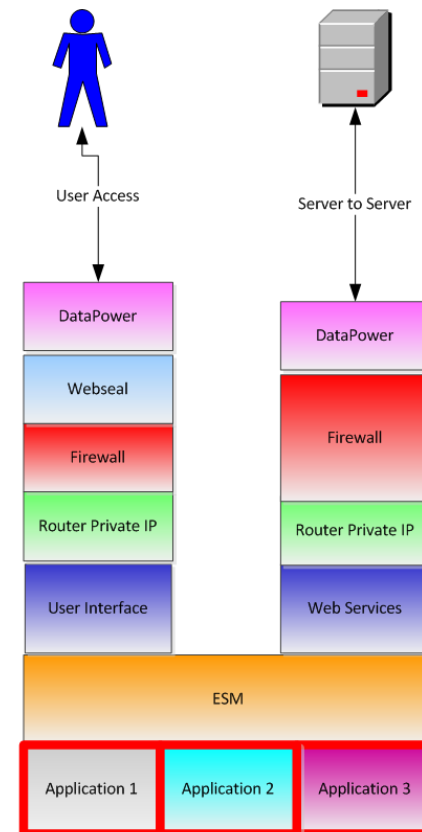
ASF Architecture



Follows NSLDSS Framework in leveraging DOD Enterprise Services

ASF Defense-in-Depth Layers

All Third Party
Traffic must go
through
ASF Security
Harness for users
and applications



ASF Implements a very extensive defense-in-depth strategy, for both human and machine interfaces

Initial Capability Screening

- IT Portfolio Manager survey possible candidates to meet requirement
- Assess the functional fit and potential costs
 - ROI of capability(ies) by “sprint” packaging
 - Cost of integration: use ASF On-Boarding Guide for ROM implementation and operational costs
- Based on trade-off analysis set up a “quick look” to manage the investment process by validating the ROI and refining the ROM costs

ASF provides a new mechanism for better DoD investment decisions

FASTER

- Documents ideal development techniques within the candidate web service or application
 - ABAC, WS Notification (JUM SDK), Data ingestion standards
 - Preferred (or standard) protocols
 - unique interfaces (least preferred/most work)
- Hosts 3rd-party capability on a hardened environment along with limited security testing
- Vendors required to use ASF install process to quickly install software in labs by utilizing Virtualization, install scripts, etc.
- Red Team Review for 3rd Party Security Integration Test
- The target time frame for any web service application is up to 30, 60, and 90 days

The On-Boarding Guide provides the processes for bringing a new capability into the ASF & assess integration complexity

ASF On-Boarding Complexity & Timelines

Higher Cost
90 Days

COST/TIME for Implementing Enterprise Services

Lower Cost
30 Days

Identity Management

Web Services Enablement

Web Services Consumability

Messaging

Documentation

Enterprise Identity Management

Enterprise Messaging

Enterprise Service Directory

Enterprise Services Management

Enterprise Collaboration

Enterprise Mediation

Level 1	Level 2	Level 3
Username/Password	Soft Cert Enabled	ABAC Enabled
XML Files	Use of Standards like WS-N, SOAP	Self Describing WSDL
XML Files	WS-I Compliant/Schema Validation	Web Services Directory enabled w/ meta data
FTP	WS-N, JMS enabled adapters	Ability to ingest unstructured data
Consultation and experts available	Source Code and test files available for testing	Step by Step Interface Documentation
Directory Server available	RBAC enabled	ABAC Enabled
No Open standards supported	Self Describing WSDLs that follow standards	Use of Standards like WS-N, SOAP, JMS
No governance model	WS-I Compliant/schema validation	Web Services Directory enabled w/ meta data
No ESM agents on Server	Currently collect OS,DB, etc metrics	Currently have ability to collect services metrics
Use of pub/sub for messaging	Currently use Sametime or other COTs for Collaborations	XMPP compliant Instant messaging
Schemas available	XSLTs available for the source system	Perform mediation on their application

ASF provides an incremental Glide Path to fully DoD compliant hosted Web Service

Typical “Quick Look” Scenario

- Scenario developed to demonstrate an initial capability, with follow-on prioritized agile sprints planned, as ROI is demonstrated
 - Target a single type of event relevant to a CCIR to discover non-obvious relationship (e.g. Terrorist activity occurring on US soil)
 - Target scenario was developed and refined using historical data via XML Repository
 - Live SIPR data contributing to the scenario, provided by JUM subscriptions
 - Further development of prototype would target other scenarios based increased data capacity and further analysis of complete data set

Scenario development will be continuously refined and expanded, given a continuing steam of data for ingestion, providing more investment decision points

- Available Third-Party capabilities vs. what was initially demonstrated
- Expected Operational Utility (value) per capability
- Expected Level of Effort (LOE) Rough Order of Magnitude (ROM) for integration, demonstration, and operations
- ROI Options on “way ahead” for IT vs. costs)
leads to more effective IT investment

DISA Typical “Quick Look” Results

A Combat Support Agency

- Ability to ingest data to the 3rd Party
- 3rd-party capability able to perform expected functions using DOD data
- Hosted 3rd-Party Web Service demonstrated as accessible by other web-services (find, bind, consume)
- Goal from brief and demo - should the department continue to fund this evolving capability?
- ROM for next set of sprints for decision by IT Portfolio Manager

3rd Party Use Case

- 3rd Party Capability
 - Integrate with ASF
 - Demo capability for ROI assessment from Community of Interest
- 3rd Party Capability doesn't have / hasn't completed:
 - An ATO
 - A NetOps Checklist
 - A Net-centric Checklist
- IT Portfolio Manager has opportunity to “try-before-they-buy”
 - Do C&A package if desired (intend to run without ASF)
 - Can request performance info for operational SLA and implement at a DECC or other DOD facility, or possibly as a Managed Service.

#1: On-board 3rd-party capability (Saffron) into the ASF security harness.

#2: Then, if it has utility, move it out of the harness when appropriate for either better performance or to lower operational

- The most important factor to make ASF, as “enabling technology”, a success is to have hosted applications that are in demand with a clear business case and scenario
 - Third Party applications that are in demand will drive innovation of new applications
 - Requirements will be better defined with end user feedback

Funding can be focused on solving business/mission needs instead of the Information Assurance posture, which is enclave provided

BACKUP SLIDES

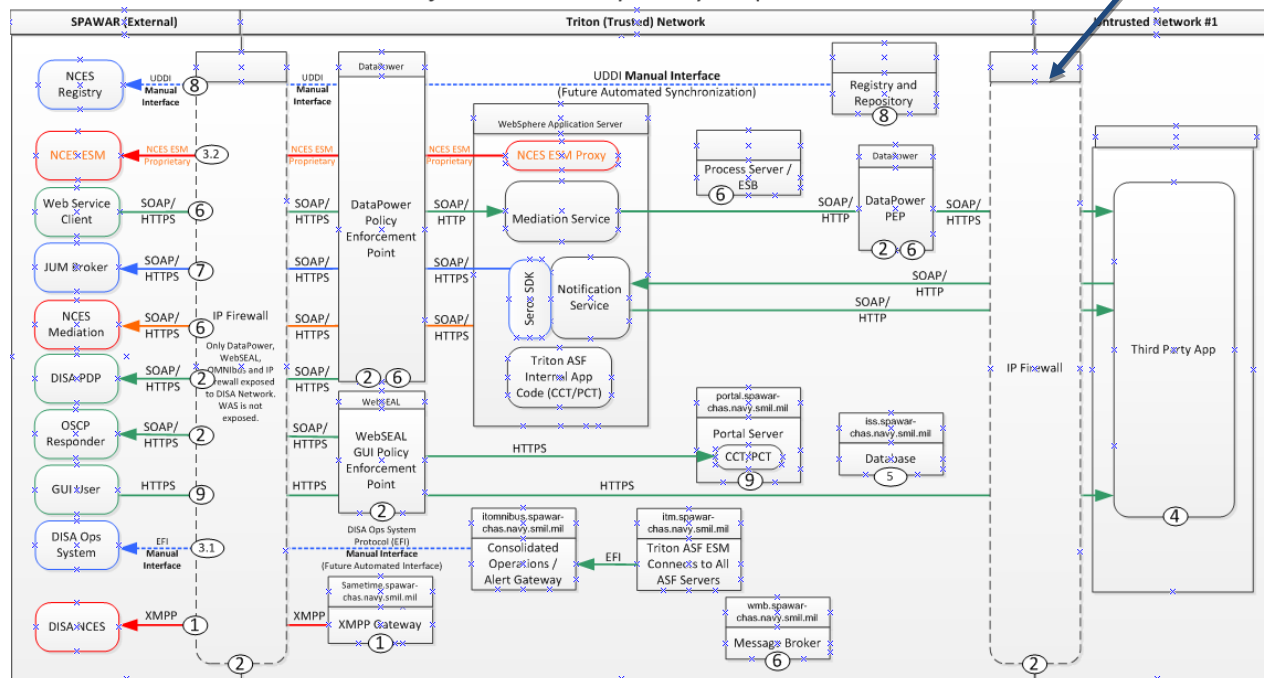
Technical Underpinnings of ASF Hosting/Isolating 3rd-Party

ASF Architecture Overview

Embedded non-routable IP Network

1. 14 Servers
Makeup ASF (all STIG hardened); normal
2. 12 Servers are on Public IP network; normal
3. **UNIQUE ELEMENT:**
2 to 10 Servers will be on the non-routable IP network (currently 2 Platforms on non-routable IP network); intent is to fully isolate the 3rd party capability and control all communications

Major DISA ASF Capability Map



DISA ASF Capabilities Mapped to Nine NCES services

NOTE: ASF Does Not Provide Service Interfaces for All These Capabilities

- 1) Collaboration (XMPP)
- 2) IA/Security (ABAC and isolation in the harness)
- 3.1) ESM - Alerts (EIF)
- 3.2) ESM - NCES ESM Proxy
- 4) Application (3rd-party hosted-web-services)
- 5) Information Management (ASF Does Not Include Significant Storage Capability)
- 6) Mediation
- 7) Messaging (JUM)
- 8) Discovery (registration and queries to UDDI and MDR)
- 9) User Interface - (ASF Does Not Include User Assistance)

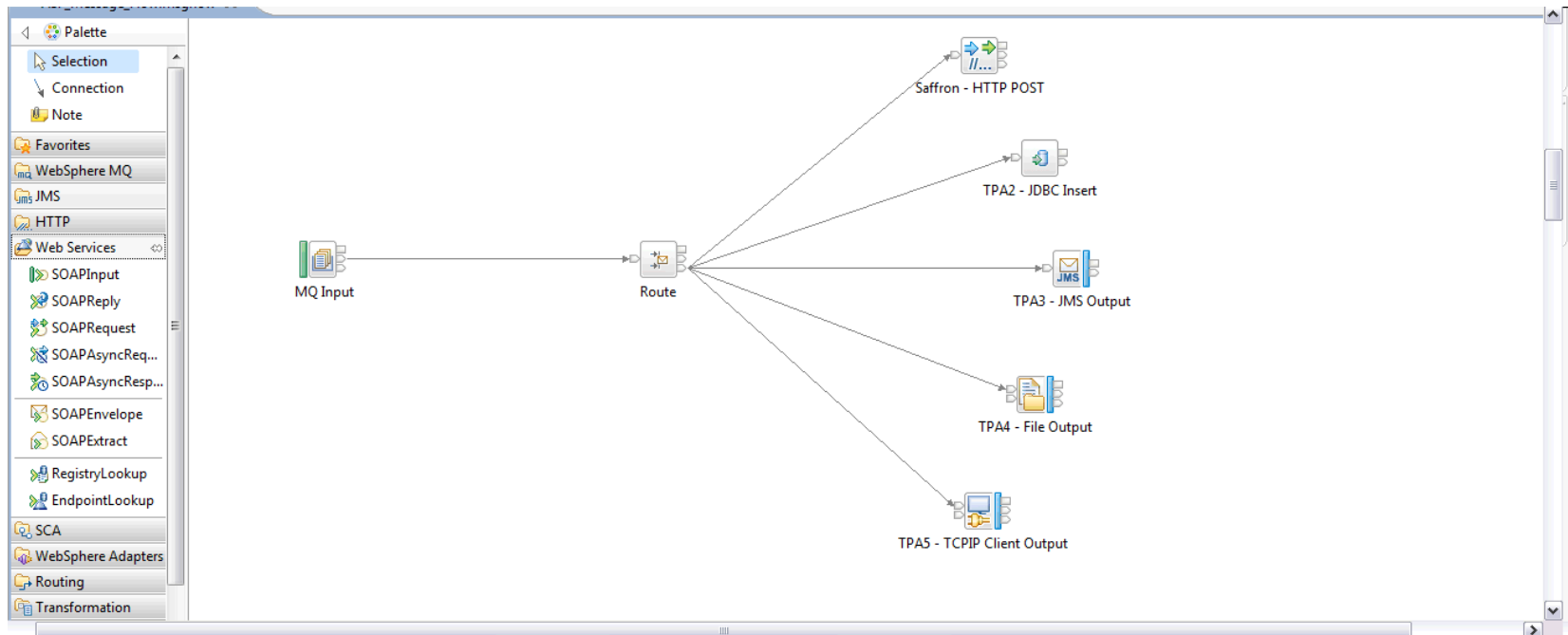
NOTE: There is only one DataPower and one IP Firewall. They are split in the diagram to clearly show the data flows. Excludes CCT/PCT data flows.

Key:

- Green** - Capability and NCES Integration is Implemented
- Blue** - Capability is implemented and is being integrated with NCES
- Red** - Capability is implemented but has not been integrated with NCES.
- Orange** - New Capability Not Yet Implemented

Message Broker APIs - Multiple Third Party Applications

- Ability to deliver messages to multiple Third Party applications
- COTS based tool for maintaining Data flows vs lines of code
- Drag and Drop Adapters for interfacing with Third party Applications
- Saffron will perform data mapping for data relationships

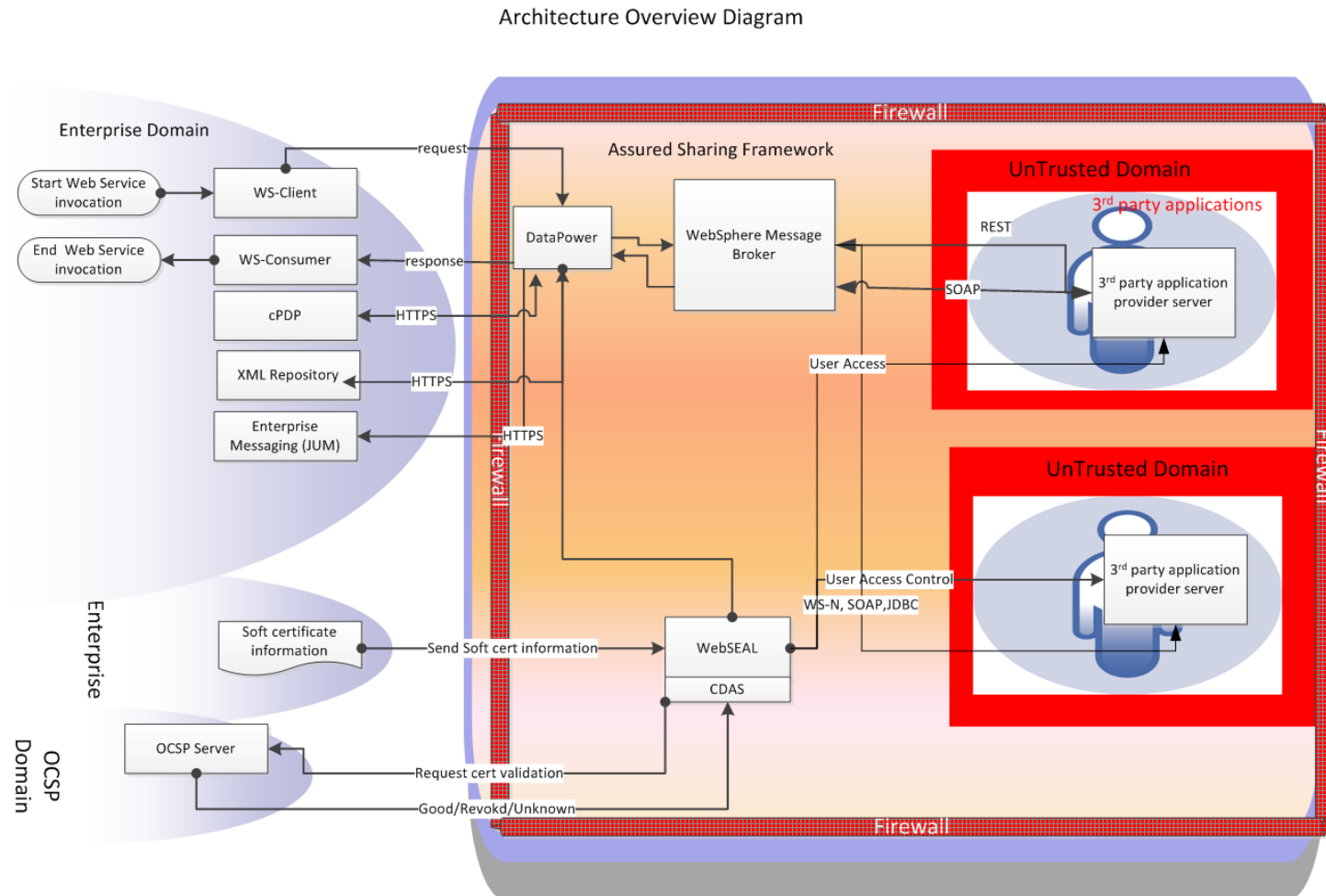


Key Enhancement: Subscription Distribution

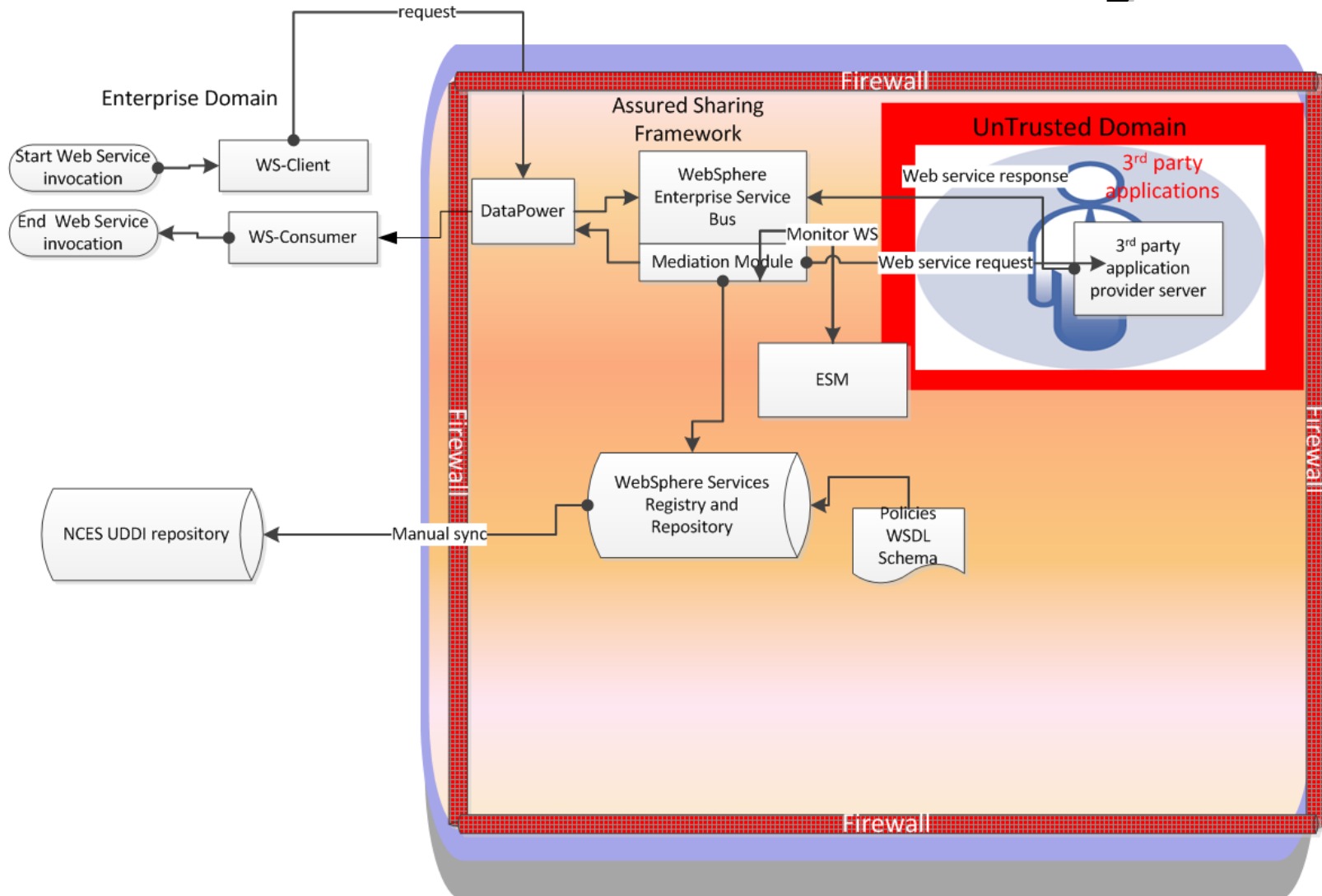
DISA ASF Overview Third Parties

A Combat Support Agency

- ASF will proxy user access and direct to appropriate third party application
- Data feeds will be distributed and delivered to third parties based on requirements
- Web Service Request will be arbitrated by ASF with individual third party applications.
- ASF will proxy asynchronous

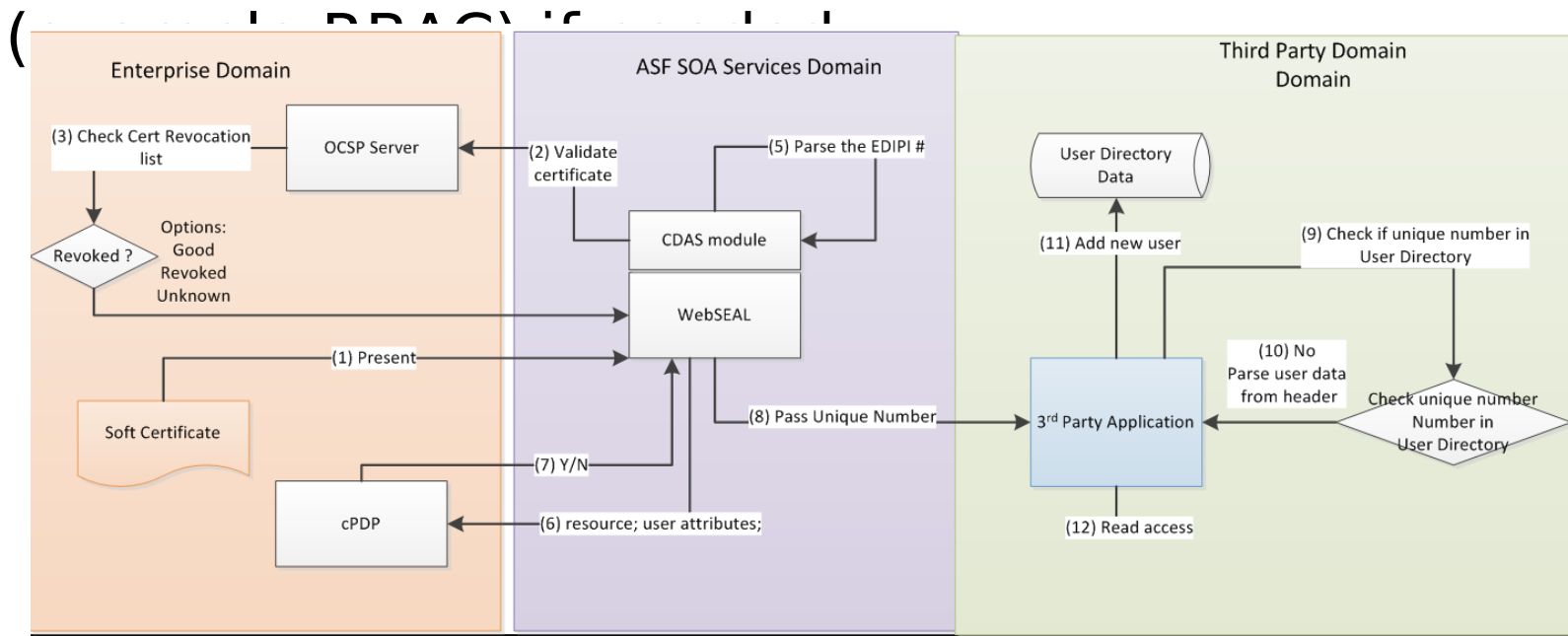


ASF Enterprise Service Discovery Flows



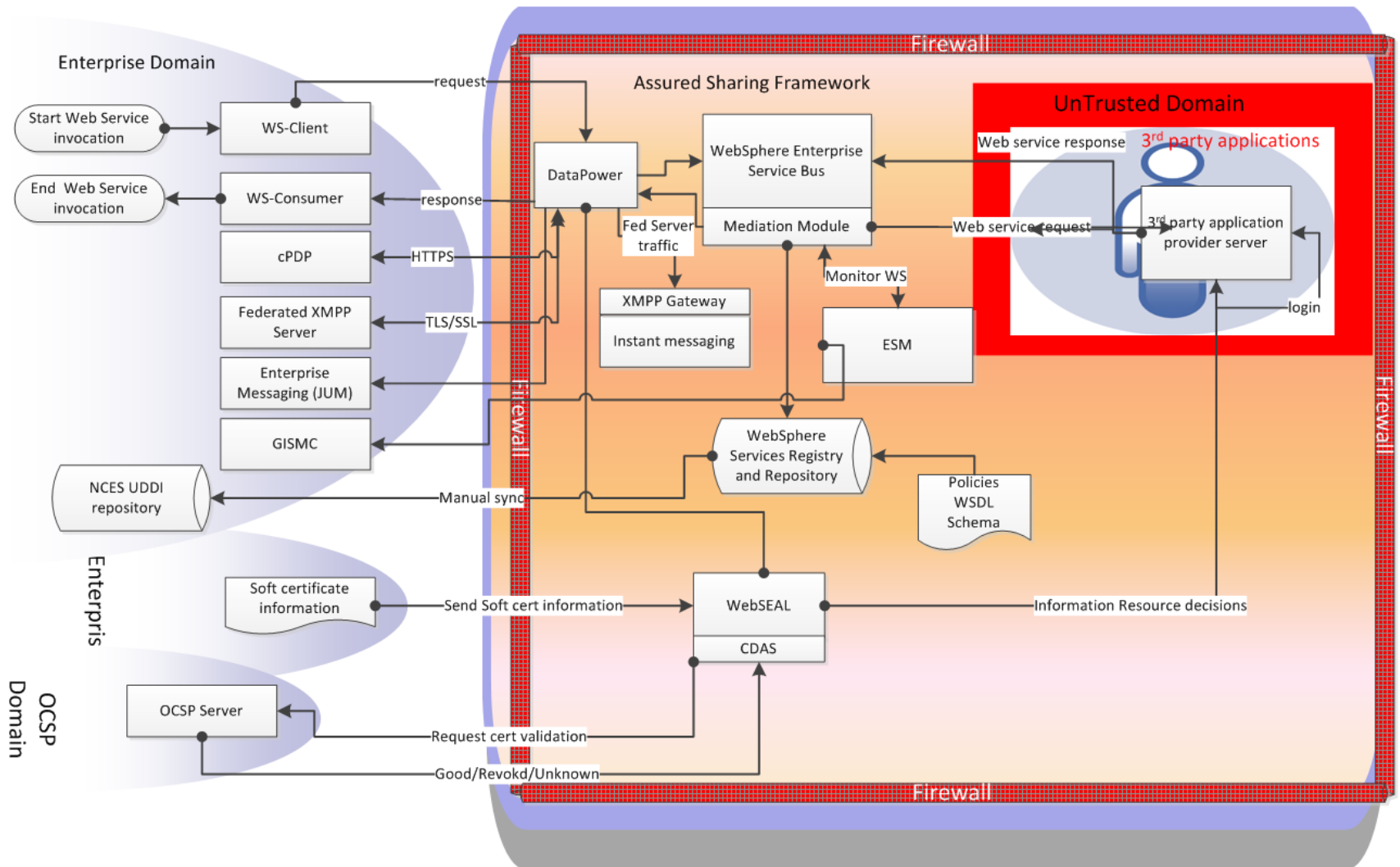
Arbitrated Enterprise Identity Management (ABAC w/CVS)

- The ASF enables CAC card or Soft Certificate access and integrates with the OCSP and cPDP
- Provides secured, arbitrated access
- Performs any necessary translation from enterprise ABAC to 3rd party application security models



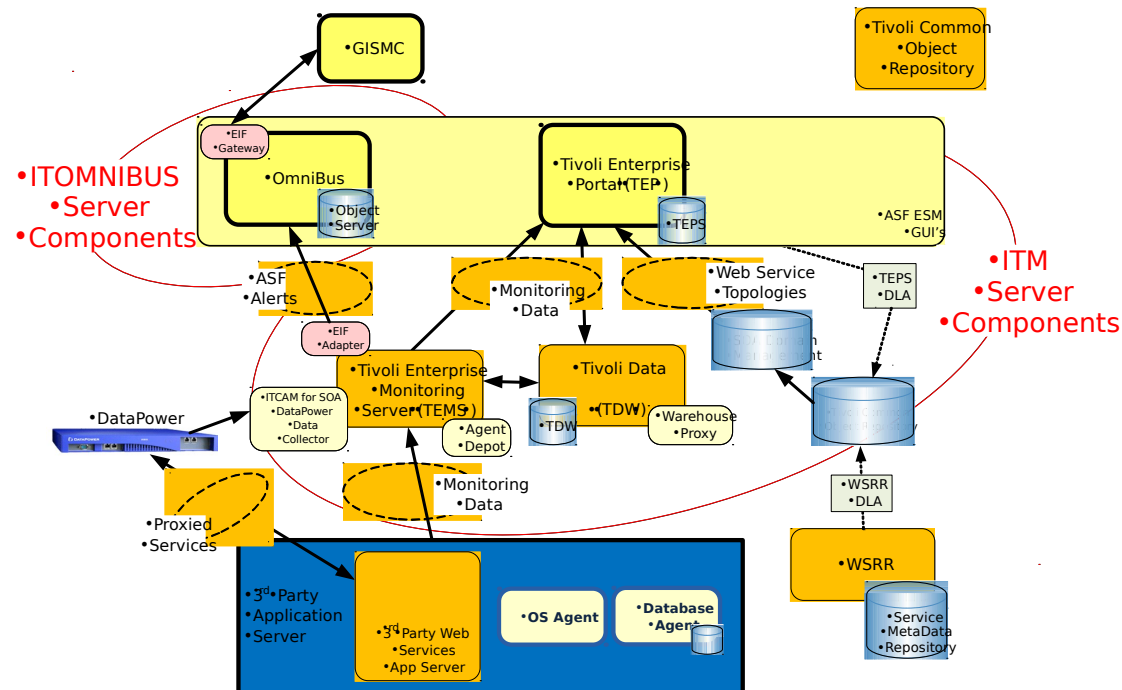
ASF Enterprise Messaging Flows

Architecture Overview Diagram



Arbitrated Enterprise Service Management (ESM)

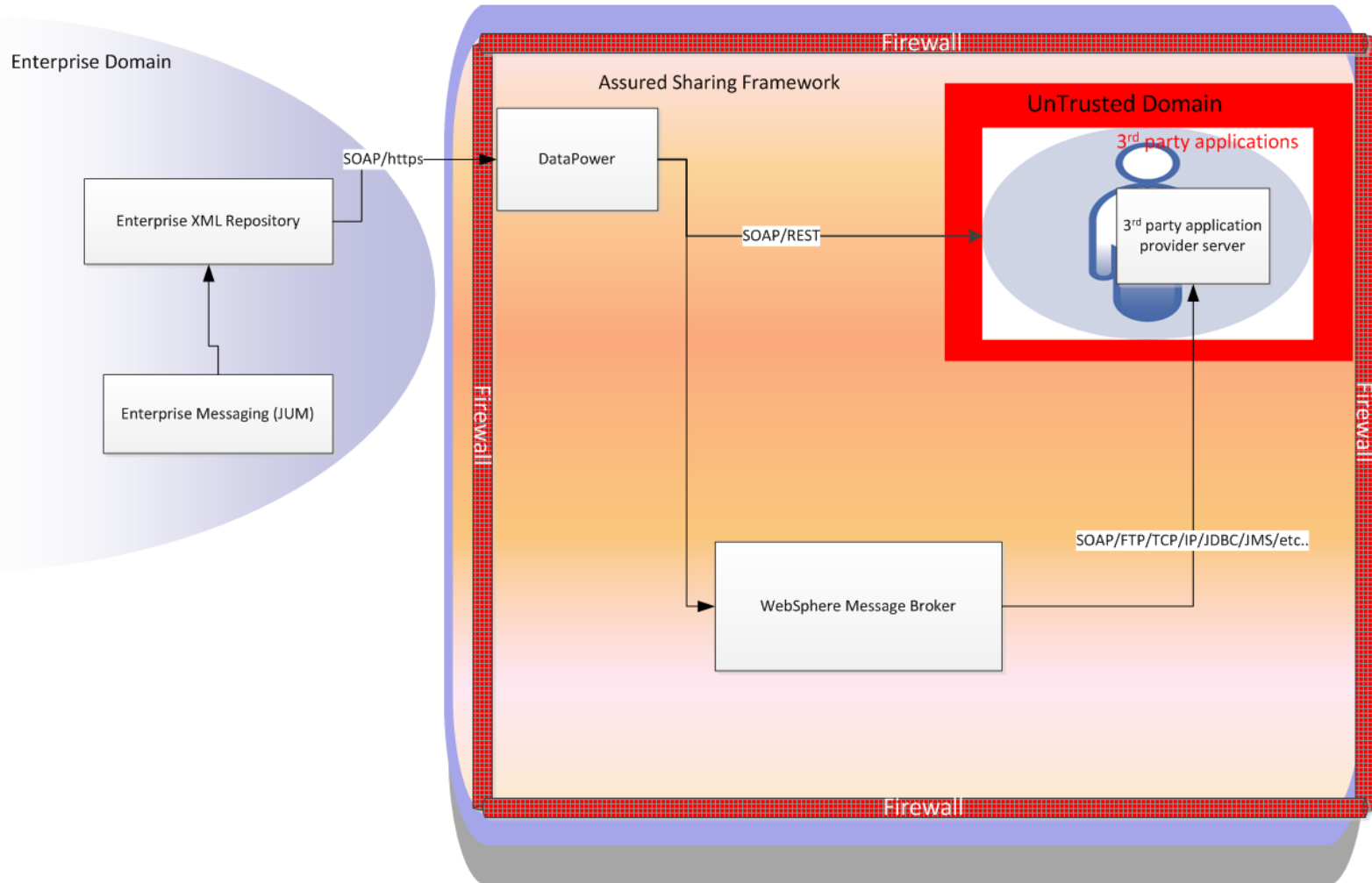
- Based on Tivoli Monitoring/NetCool/Omnibus
- Internal monitoring
 - Status of Triton Environment
 - Web Services Health Status
 - 3rd Party Health Status
- External monitoring
 - Situation Alert forwarded Outside of Triton
- The ASF supports integrated rolled up monitoring when supported at the enterprise level



ASF Enterprise Content Discovery (XML-Repository)

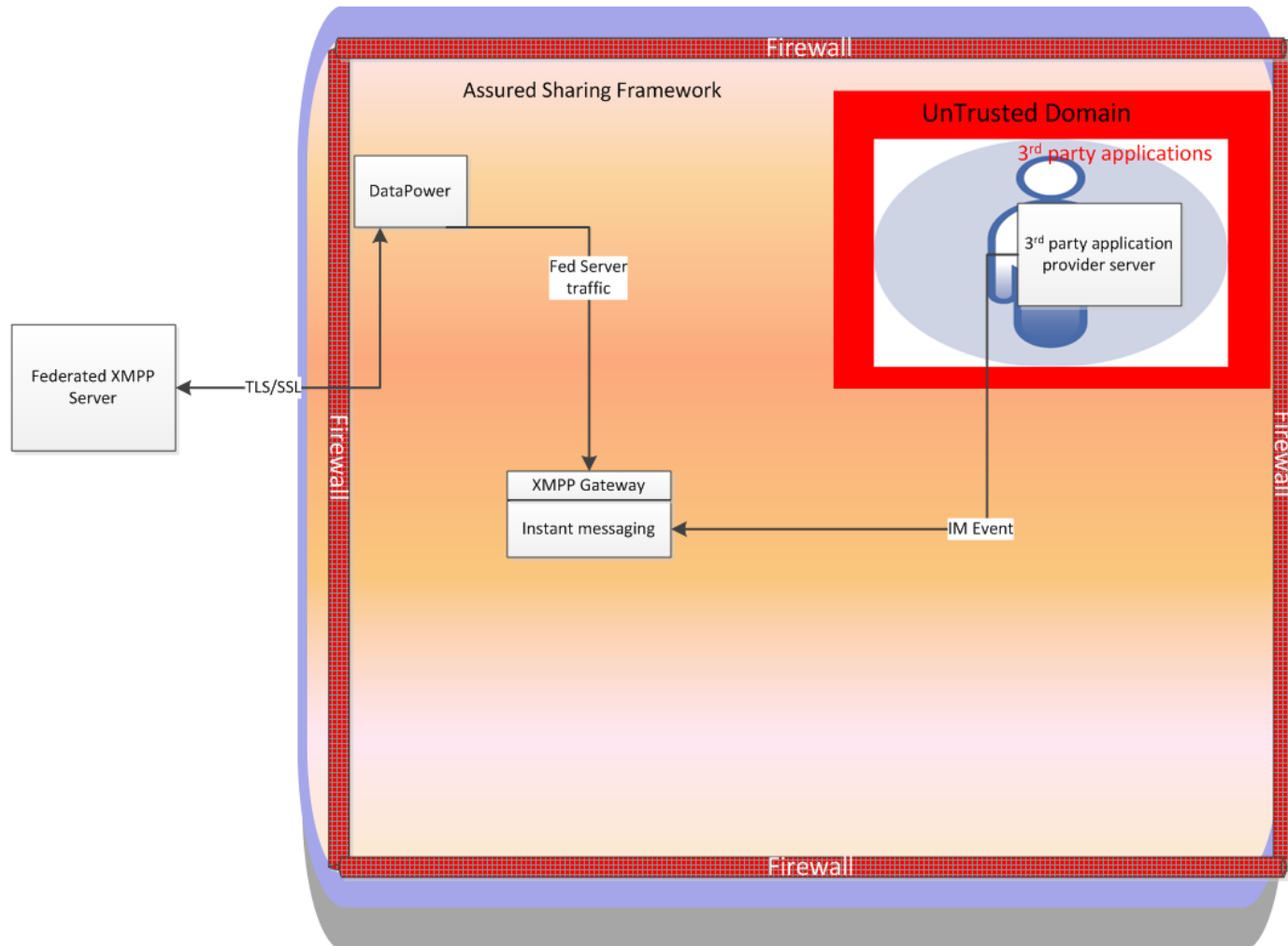
Elements

XML Repository Data Flows



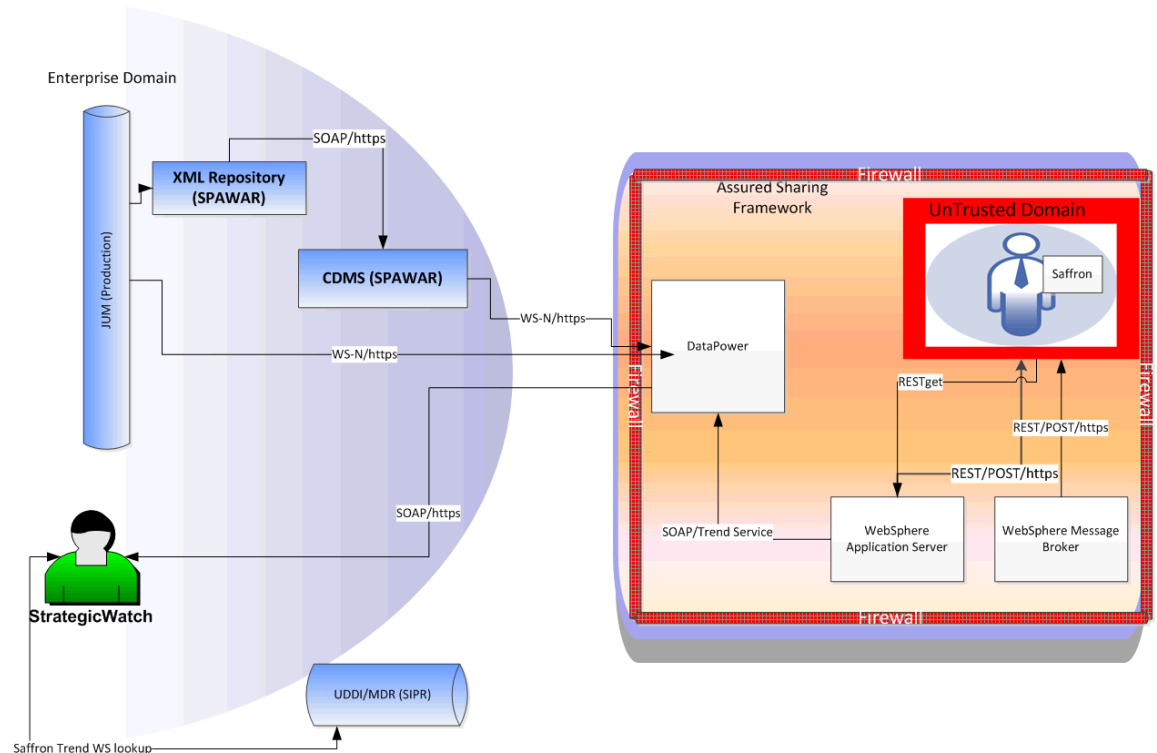
ASF Federated Enterprise Collaboration (XMPP-Chat)

Flows



- 3rd-Party is seeded with historical data in MarkLogic and CDMS performs translation (event driven arbitration).
- Live Data feeds from JUM are posted to Saffron (pub/sub arbitration).
- 3rd-Party Web-Service is exposed by ASF (request/response arbitration).
- Approximately 10-12 day integration effort

Saffron ASF Integration



BACKUP SLIDES

- Add Production Readiness to trade-space
- Add Operational Cost Driver to trade-space
- Add more graphical user interfaces for DOD integrator (SPAWAR)

**Key element for IT Efficiencies &
Alignment with DISA's Lines of Operations**

- Managed Service for some business lines like the Intel Community
- Support to other missions via SPAWAR pre-production pipeline and DECC for operations
- DECC operations for Communities of Interest that have their own pre-production pipeline
- Integrate offerings with RACE and FORGE
- PMO for CCB and needed upgrades (pre-production and operations)
- Community of Interest targets: Command and Control, Combat Support, Modeling and Simulation of Weapons Systems, DoD Business Systems

ASF provides a new architectural component to better secure the DoD

Links to DISA Campaign Plan

A Combat Support Agency

- **Acquisition**

- TSK 2.1.1.1.3 – BAA lessons learned;
- TSK 2.1.1.2.1 – Agile development;
- TSK 2.1.1.2.1 – also agile development;
- TSK 2.1.3.1.1, 2.1.3.1.2, and 2.1.3.1.3 – architectural tenets and migration plans;
- TSK 2.1.4.1.5 – train workforce for agile development) ;

- **Engineering**

- TSK 2.3.1.2.2 – JCTD best practices;
- TSK 2.3.2.1.1 – dev/demo environment;
- TSK 2.3.2.1.1 – quick look analysis;
- TSK 2.3.2.1.4 – partnership and accelerated delivery;
- TSK 2.3.2.1.5 – engineering best practices for innovation while managing the residual risk;
- TSK 2.3.2.1.6 – eval/expand dev/demo avenues;
- TSK 2.3.3.1.2 – Identity and access Mgt tools for FORGE;
- TSK 2.3.3.2.1 – test environment for FORGE;
- TSK 2.3.3.2.2 – perf/scale/reliability testing environment for FORGE;
- TSK 2.3.3.2.3 – virtual net-centric test environment w/Joint Base Concept at SPAWAR-ATLANTIC;
- TSK 2.3.3.4.1 – promote validated demo to production;
- TSK 2.4.3.2.1 – process for promote to production with Service Level Mgmt;
- TSK 2.4.3.2.3 – "fault-isolation and response" triage for promotion to production;
- TSK 2.4.3.2.5 – release mgmt/graduation/promotion process;
- TSK 2.4.3.5.1 – standardized DOD (SPAWAR) Service Level Agreements for OCTO;
- TSK 2.4.3.5.2 – standard DISA SLAs for OCTO projects);

- **Planning**

- TSK 2.6.1.2.1 – single campaign plan for COCOM support and IT efficiency goals;
- TSK 2.6.2.1.7 – corporate level contract strategy for BAA use); and

- **Testing**

- TSK 2.9.1.2.1 – virtualize testing/demo capabilities for FORGE;
- TSK 2.9.2.1.6 – quick start user stories/use cases;
- TSK 2.9.2.1.12 – agile T&E for MUA/OUA;
- TSK 2.9.2.11.15 – agile IA/CND built-into security test harness;
- TSK 2.9.3.1.4 – live, virtual, and constructive distributed dev/demo environment with SPAWAR-ATLANTIC and other sites thru Joint Base initiative).